



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Helena Handschuh

Application No.: 09/774,674

Filing Date: February 1, 2001

Group Art Unit: 2134

Examiner: Jacob Lipman

Confirmation No.: 3521

Title: A COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT USING A PUBLIC KEY
CRYPTOGRAPHY ALGORITHM ON AN ELLIPTIC CURVE

AMENDMENT/REPLY TRANSMITTAL LETTER

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Enclosed is a reply for the above-identified patent application.

☐ A Petition for Extension of Time is also enclosed.

☐ Terminal Disclaimer(s) and the ☐ \$55.00 (2814) ☐ \$110.00 (1814) fee per
Disclaimer due under 37 C.F.R. § 1.20(d) are also enclosed.

☐ Also enclosed is/are _____

☐ Small entity status is hereby claimed.

☐ Applicant(s) requests continued examination under 37 C.F.R. § 1.114 and enclose the
☐ \$395.00 (2801) ☐ \$790.00 (1801) fee due under 37 C.F.R. § 1.17(e).

☐ Applicant(s) requests that any previously unentered after final amendments not be entered.
Continued examination is requested based on the enclosed documents identified above.

☐ Applicant(s) previously submitted _____

on _____,
for which continued examination is requested.

☐ Applicant(s) requests suspension of action by the Office until at least _____,
which does not exceed three months from the filing of this RCE, in accordance with 37 C.F.R.
§ 1.103(c). The required fee under 37 C.F.R. § 1.17(i) is enclosed.

☐ A Request for Entry and Consideration of Submission under 37 C.F.R. § 1.129(a) (1809/2809) is also
enclosed.

- ☒ No additional claim fee is required.
- ☐ An additional claim fee is required, and is calculated as shown below.

AMENDED CLAIMS					
	No. of Claims	Highest No. of Claims Previously Paid For	Extra Claims	Rate	Additional Fee
Total Claims		MINUS =	0	x \$18.00 (1202) =	\$ 0.00
Independent Claims		MINUS =	0	x \$88.00 (1201) =	\$ 0.00
If Amendment adds multiple dependent claims, add \$300.00 (1203)					
Total Claim Amendment Fee					\$ 0.00
<input type="checkbox"/> Small Entity Status claimed - subtract 50% of Total Claim Amendment Fee					\$ 0.00
TOTAL ADDITIONAL CLAIM FEE DUE FOR THIS AMENDMENT					\$ 0.00

- ☐ A check in the amount of _____ is enclosed for the fee due.
- ☐ Charge _____ to Deposit Account No. 02-4800.
- ☐ Charge _____ to credit card. Form PTO-2038 is attached.

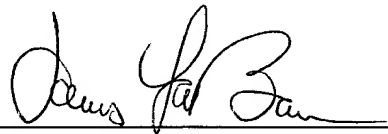
The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17, 1.20(d) and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800. This paper is submitted in duplicate.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: November 10, 2004

By 
James A. LaBarre
Registration No. 28,632



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)
Helena Handschuh) Group Art Unit: 2134
Application No.: 09/774,674) Examiner: Jacob Lipman
Filed: February 1, 2001) Confirmation No.: 3521
For: A COUNTERMEASURE METHOD)
IN AN ELECTRONIC COMPONENT)
USING A PUBLIC KEY)
CRYPTOGRAPHY ALGORITHM ON)
AN ELLIPTIC CURVE)

REQUEST FOR RECONSIDERATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action dated August 12, 2004, Applicant respectfully requests reconsideration and withdrawal of the rejections of the claims.

Claims 1, 2 and 13 were rejected under 35 U.S.C. §102, on the grounds that they were considered to be anticipated by the *Miyazaki et al.* reference (U.S. 6,477,254). In addition, claims 3-12 were rejected under 35 U.S.C. §103, as being unpatentable over the *Koblitz* publication entitled "A Course in Number Theory and Cryptography", in view of the *Miyazaki* reference. It is respectfully submitted that the *Miyazaki* reference neither discloses, nor otherwise suggests, the claimed subject matter, whether considered by itself or in combination with the *Koblitz* reference.

The claimed invention is directed to a countermeasure that protects against the ability of an unauthorized person to determine a private encryption/decryption key. As